BẢN TIN NỘI BỘ

CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Giả danh công an phát tán mã độc đòi tiền chuộc nghìn USD

GandCrab 5.2 là phiên bản mới trong họ Mã độc tống tiền GandCrab lan rộng trên toàn cầu trong hơn một năm qua. Ngày 5/4/2018, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đã phát hành Công văn số 58/VNCERT-ĐPƯC về việc ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab (phiên bản 1.0 và 2.0) và hiện nay cũng đã hỗ trợ giải mã GandCrab phiên bản 5.1 trở về trước.

Tuy nhiên, hiện nay qua theo dõi không gian mạng, Trung tâm VNCERT phát hiện từ giữa tháng 3/2019 đến nay đang có chiến dịch phát tán Mã độc tống tiền GandCrab 5.2 vào Việt Nam và các nước Đông Nam Á.

Tại Việt Nam, GandCrab 5.2 được phát tán thông qua thư điện tử giả mạo từ Bộ Công an Việt Nam với tiêu đề "Goi trong Cong an Nhan dan Viet Nam", có đính kèm tệp documents.rar.

Khi người dùng giải nén và mở tệp tin đính kèm, mã độc sẽ được kích hoạt và toàn bộ dữ liệu người dùng bị mã hóa, đồng thời sinh ra môt tệp nhằm yêu cầu và hướng dẫn người dùng trả tiền chuộc từ 400 - 1.000 USD bằng cách thanh toán qua đồng tiền điện tử để giải mã dữ liệu.

Trước tình hình này, Trung tâm VNCERT đưa ra khuyến nghị cần theo dõi, ngăn chặn kết nối đến các máy chủ máy chủ điều khiển mã độc tống tiền GandCrab và cập nhật vào các hệ thống bảo vệ như: IDS/IPS, Firewall,… Trong trường hợp phát hiện sự cố, cần nhanh chóng cô lập vùng/máy đã phát hiện.

Các đơn vị chuyên trách về ATTT cần thông báo để người sử dụng nâng cao cảnh giác, không mở và click vào các liên kết cũng như các tập tin đính kèm trong email có chứa các tập tin dạng .doc, .pdf, .zip, rar,… được gửi từ người lạ. Đó cũng có thể là một email được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường.

Theo Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, mã độc tống tiền GandCrab rất nguy hiểm. Nó có thể đánh cắp thông tin và mã hóa toàn bộ dữ liệu trên máy bị nhiễm. Tin tặc khai thác và tấn công sẽ gây lên nhiều hậu quả nghiêm trọng khác.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần nâng cao cảnh giác, không mở và click vào các liên kết cũng như các tập tin đính kèm trong email có chứa các tập tin dạng .doc, .pdf, .zip, rar,… được gửi từ người lạ hoặc các từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/canh-bao-ma-doc-tong-tien-moi-gandcrab-qua-email-513895.html

2. Adobe phát hành bản vá cho các lỗ hổng nghiêm trọng trong Photoshop CC và Digital Edition

Khai thác thành công, cả hai lỗ hổng nghiêm trọng có thể cho phép kẻ tấn công thực thi mã tùy ý bằng các đặc quyền người dùng và kiểm soát hệ thống bị ảnh hưởng.

Tuy nhiên, Adobe cho hay công ty chưa phát hiện các trường hợp khai thác trên thực tế.

Lỗ hổng trong Adobe Photoshop CC (CVE-2019-7094), do Trend Micro Zero Day Initiative phát hiện, là một lỗi vùng nhớ heap có ảnh hưởng đến Photoshop CC 19.1.7 và các phiên bản 19.x trước đó cũng như Photoshop CC 20.0.2 và Phiên bản 20.x trở về trước cho hệ điều hành Microsoft Windows và Apple macOS.

Người dùng được khuyến nghị cập nhật phần mềm của họ lên Adobe Photoshop CC phiên bản 19.1.8 và Photoshop CC phiên bản 20.0.4 cho Windows và macOS.

Một lỗ hổng nghiêm trọng khác, CVE-2019-7095, nằm trong chương trình phần mềm đọc sách điện tử của công ty, Adobe Digital Edition, là một lỗ hổng tràn bộ nhớ heap ảnh hưởng đến phiên bản 4.5.10.185749 và thấp hơn cho hệ điều hành Microsoft Windows.

Người dùng nên cập nhật phần mềm của họ lên phiên bản Adobe Digital Edition 4.5.10.186048.

Cả hai bản cập nhật đều được xếp hạng ưu tiên là 3, có nghĩa là các lỗ hổng được xử lý trong các bản cập nhật khó có thể bị khai thác trong các cuộc tấn công, theo lưu ý của Adobe.

Đầu tháng 3 này, Adobe cũng đã tung ra bản cập nhật vá khẩn cấp lỗ hổng thực thi mã tùy ý nghiêm trọng (CVE-2019-7816) trong nền tảng phát triển ứng dụng web ColdFusion đang bị khai thác tích cực trên thực tế.

Do đó, người dùng phần mềm Adobe bị ảnh hưởng cho các hệ thống Windows và macOS được khuyến khích cập nhật các gói phần mềm lên các phiên bản mới nhất càng sớm càng tốt.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người sử dụng trên Windows và macOS cần cập nhật phiên bản mới nhất của Adobe Photoshop CC và Digital Edition để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/adobe-phat-hanh-ban-va-cho-cac-lo-hong-nghiem-trong-trong-photoshop-cc-va-digital-edition.12050/

3. Microsoft phát hành Patch Tuesday tháng 3, vá 64 lỗ hổng – hai lỗi đang bị khai thác

Microsoft vừa phát hành bản cập nhật Patch Tuesday tháng 3 năm 2019, giải quyết tổng cộng 64 lỗ hổng an ninh trong hệ điều hành Windows và các sản phẩm khác. Trong đó, 17 lỗi được đánh giá nghiêm trọng, 45 lỗi quan trọng, một lỗi mức trung bình và một lỗi mức độ nghiêm trọng thấp.

Bản cập nhật khắc phục các lỗi trong Windows, Internet Explorer, Edge, MS Office và MS Office SharePoint, ChakraCore, Skype for Business và Visual Studio NuGet.

Bốn lỗ hổng quan trọng được vá tháng này đều đã được công khai, nhưng chưa bị khai thác trong thực tế.

Microsoft cũng vá hai lỗ hổng leo thang đặc quyền zero-day trong Windows.

Cả hai lỗ hổng, đều được đánh giá quan trọng, nằm trong thành phần Win32k mà tin tặc đang tích cực khai thác trong thực tế, bao gồm một lỗi mà Google đã cảnh báo vào tuần trước.

Tuần trước Google phát hành một bản cập nhật quan trọng cho trình duyệt Chrome để khắc phục một lỗi nghiêm trọng (CVE-2019-5786) mà nếu khai thác cùng với lỗ hổng trong Windows (CVE-2019-0808).

Khai thác thành công đồng thời cả hai lỗ hổng cho phép kẻ tấn công từ xa thực thi mã tùy ý trên các máy tính mục tiêu chạy Windows 7 hoặc Server 2018 và kiểm soát hoàn toàn.

Lỗ hổng leo thang đặc quyền zero-day thứ hai trong Windows, CVE-2019-0797, cũng được khai thác trong thực tế tương tự như lỗ hổng đầu tiên nhưng ảnh hưởng đến Windows 10, 8.1, Server 2012, 2016 và 2019.

Gần như tất cả các lỗ hổng nghiêm trọng đều dẫn đến tấn công thực thi mã từ xa và chủ yếu ảnh hưởng đến các phiên bản của Windows 10 và Server. Hầu hết các lỗ hổng này nằm trong Chakra Scripting Engine, VBScript Engine, DHCP Client và IE.

Một số lỗ hổng quan trọng cũng dẫn đến tấn công thực thi mã từ xa, một số khác cho phép leo thang đặc quyền, tiết lộ thông tin và các cuộc tấn công từ chối dịch vụ.

Người dùng và quản trị viên hệ thống được khuyến cáo cập nhật các bản vá mới nhất càng sớm càng tốt để ngăn chặn tin tặc và tội phạm mạng kiểm soát hệ thống của họ.

Để cài đặt các bản cập nhật vá an ninh mới nhất, vào Settings → Update & Security → Windows Update → Check for updates hoặc bạn có thể cài đặt các bản cập nhật theo cách thủ công.

Để giải quyết các cập nhật có vấn đề trên Windows 10, Microsoft đã giới thiệu một biện pháp an toàn là tự động gỡ các bản cập nhật phần mềm bị lỗi được cài đặt trên hệ thống nếu hệ điều hành phát hiện lỗi khởi động.

Vì vậy, sau khi cài đặt bản cập nhật tháng này, nếu bạn nhận được thông báo sau trên thiết bị của mình, máy tính Windows 10 của bạn đã được khôi phục từ một lỗi khởi động và hệ điều hành đã khắc phục lỗi đó bằng cách gỡ cập nhật Windows được cài đặt gần đây.

"Chúng tôi đã xóa một số cập nhật được cài đặt gần đây để khôi phục thiết bị của bạn từ lỗi khởi động".

Windows 10 sau đó sẽ tự động chặn cài đặt bản cập nhật có vấn đề đó trong 30 ngày.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị viên cần cập nhật các bản vá mới nhất ngay lập tức để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/microsoft-phat-hanh-patch-tuesday-thang-3-va-64-lo-hong-%E2%80%93-hai-loi-dang-bi-khai-thac.12055/

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Apache	CVE-2019-0187 CVE-2019-0192 CVE-2018-11793 ...	Nhóm 06 lỗ hổng trong một số sản phẩm của Apache (JMeter, Solr, Qpid Broker-J, Apache Traffic Server) cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn và thực thi mã lệnh trong phạm vi của ứng dụng.	Đã có thông tin xác nhận và bản vá
2	Apple	CVE-2019-6213 CVE-2019-6218 CVE-2019-6235 ...	Nhóm 30 lỗ hổng trên các sản phẩm của Apple (iOS, macOS, tvOS, watchOS, iTunes, iCoud, Safari) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau. Nhiều lỗ hổng cho phép khai thác lỗi tràn bộ đệm, chèn và thực thi mã lệnh với quyền của hệ thống và đã có mã khai thác (như CVE-2019-6213, CVE-2019-6218...).	Đã có thông tin xác nhận và bản vá Một số lỗ hổng đã có mã khai thác
3	Microsoft	CVE-2019-0606 CVE-2019-0673 CVE-2019-0623	Nhóm 75 lỗ hổng trên nhiều sản phẩm của Microsoft (.NET Framework, Microsoft Edge, Exchange Server, Internet Explorer, Office Access Connectivity Engine, SharePoint) cho phép đối tượng tấn công thực hiện thu thập thông tin nhạy cảm trên hệ thống, thực thi mã lệnh và tấn công leo thang.	Đã có thông tin xác nhận và bản vá
4	Cisco	CVE-2019-1591 CVE-2019-1593 ...	Nhóm 20 lỗ hổng trên một số sản phẩm của Cisco (các dòng switch Nexus, NX-OS, FXOS Software,) cho phép truy cập và thông tin nhạy cảm lưu trữ trên hệ thống, chèn và thực thi	Đã có thông tin xác nhận và bản vá.

			mã lệnh để chiếm quyền kiểm soát thiết bị.	
5	Jenkins	CVE-2019- 1003034 CVE-2019-1003039 CVE-2019-1003030 ...	Nhóm 11 lỗ hổng trên phần mềm Jenkins (phần mềm sử dụng trong phát triển phần mềm) cho phép đối tượng tấn công thu thập thông tin xác thực lưu trữ trong cấu hình của Plugin, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	plpanaifheaighai.com
2	n.hmiblgoja.ru
3	ajkeahkcueafuiaeuf.ru
4	mokoaehaeihgiaheih.ru
5	iuefgauiaiduihgs.com
6	43trfdsds.com
7	mel.cloudcontentsmak.com
8	https://yourcherrychicks.com/xefyzznumsa
9	d3s1.me
10	bszotsjovih.com

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:

- Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
- Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.